Caicedo, Y. 2013. Problema de suma cero: la conjetura de Kemnitz. Revista Sigma,11(1).Pág 39-50 http://coes.udenar.edu.co/revistasigma/articulos/articulosX/1.pdf

REVISTA SIGMA
Departamento de Matemáticas
Universidad de Nariño

Volumen XI Nº 1 (2013), páginas 39–50

Problema de suma cero: la conjetura de Kemnitz

Yadira Caicedo Bravo[1]

Abstract. In 1961, P. Erdös, A. Ginzburg and A. Ziv proved that "any sequence of $(2n-1)$ integers contains a subsequence of size n whose sum of elements is divisible by n". This result was extended to several dimensions; for example, the two-dimensional case consists in determining the smallest integer $s = s(n, 2)$ such that any sequence with s elements of $\mathbb{Z}_n \oplus \mathbb{Z}_n$ contains a subsequence of size n whose sum of elements it is congruent with zero module n. In 1983, A. Kemnitz conjectured that $s(n, 2) = 4n - 3$ for all n. This conjecture was an open problem during 20 years. However, in October of 2003, C. Reiher proved that it is true. In this work we present the detailed proof of the function value $s(n, 2)$ for $n = 2, 3, 5$ and we rebuilt the prove of the Kemnitz Conjecture, well-known today as the Theorem of Kemnitz-Reiher.

Keywords. Kemnitz, Chevalley-Warning, zero sum.

Resumen. En 1961, P. Erdös, A. Ginzburg y A. Ziv demostraron que "toda secuencia de $(2n - 1)$ enteros contiene una subsecuencia de tamaño n cuya suma de elementos es divisible entre n." Este resultado fue extendido a varias dimensiones; por ejemplo, el caso bidimensional consiste en determinar el menor entero $s = s(n, 2)$ tal que cualquier secuencia con s elementos de $\mathbb{Z}_n \oplus \mathbb{Z}_n$ contiene una subsecuencia de tamaño n, cuya suma de elementos es congruente con cero módulo n. En el año de 1983, A. Kemnitz conjeturó que $s(n, 2) = 4n - 3$, para todo n. Esta conjetura fue un problema abierto durante 20 años hasta que, en Octubre de 2003, C. Reiher probó que es verdadera. En este trabajo presentamos la demostración en detalle del valor de la función $s(n, 2)$ para los valores de $n = 2, 3, 5$ y luego realizamos la reconstrucción de la demostración de la Conjetura de Kemnitz, conocida hoy como el Teorema de Kemnitz-Reiher.

Palabras Clave. Kemnitz, Chevalley-Warning, suma cero.

Introducción

La Conjetura de Kemnitz surge a partir del problema unidimensional conocido como el Teorema de Erdös, Ginzburg y Ziv [6]. Existen varias demostraciones de este resultado y algunas generalizaciones; por ejemplo, el primero que se interesó por estudiar el problema general fue H. Harborth [9] en el año de 1973, quien enunció el problema de la siguiente manera.
Sea $\mathbb{Z}_n^d$ la suma directa de d copias del grupo aditivo $\mathbb{Z}_n$ de enteros módulo n, sea $s(n, d)$ el menor entero s tal que cualquier secuencia con s elementos de $\mathbb{Z}_n^d$ contiene una subsecuencia

[1]Corresponding author: Departamento de Matemáticas, Facultad de Ciencias Naturales y Exactas, Universidad del Valle, Cali, Colombia. e-mail: yadira0427@gmail.com

de tamaño n cuya suma de elementos es congruente con cero módulo n, el problema consiste en hallar $s(n,d)$ con la propiedad descrita.
La existencia de este número se puede garantizar por las cotas triviales demostradas por H. Harborth [9]:

$$(n-1)2^d + 1 \leq s(n,d) \leq (n-1)n^d + 1. \tag{0.1}$$

Se conoce que $s(n,1) = 2n-1$ (Teorema de Erdös, Ginzburg y Ziv). Kemnitz en [10] conjeturó en el año de 1983 que $s(n,2) = 4n-3$ para todo n, demostró además que para los casos $n = 2,3,5,7$ la conjetura es verdadera y por lo tanto para todo n de la forma $n = 2^a 3^b 5^c 7^d$, donde a,b,c,d son enteros no negativos [10].
Esta conjetura fue un problema abierto durante 20 años y en Octubre de 2003, C. Reiher en [13], probó que es verdadera.
Los resultados anteriormente mencionados hacen parte de la Teória de Suma Cero. La Teoría de Suma Cero, que surge a partir de los problemas de suma cero, es un tema de frontera en la investigación actual. En la Teoría de Números Combinatoria los problemas de suma cero, los conjuntos suma y los cubrimientos de los enteros son tres diferentes tópicos iniciados por P. Erdös e investigados por muchos autores; éstos juegan un papel importante en la Teoría de Números y Combinatoria, existe una conexión profunda de estas tres áreas aparentemente no relacionadas y tienen por objeto establecer una teoría unificada, además tiene aplicaciones en muchos aspectos de campos finitos y Teoría de Grafos. También los problemas de suma cero tienen relación con la Teoría de Ramsey en el estudio sobre los números Ramsey de suma cero y con la Teoría de Códigos.

1. Valor de la función $s(p,2)$ para $p = 2$ y $p = 3$

En esta sección vamos a mostrar que $s(p,2) = 4p-3$, para los casos cuando $p = 2$ y $p = 3$ analizando el problema desde un punto de vista geométrico con base en el texto [7], en el cual se describe este problema como una aplicación del Principio del Palomar (También llamado Principio de Dirichlet o de las cajas), que en su versión más sencilla afirma que: *si $k+1$ objetos son repartidos en k casillas entonces al menos una casilla debe contener por lo menos dos objetos.*; sin embargo la versión que usaremos en este trabajo es la siguiente, la cual está demostrada en [7]:

Teorema 1.1. Sean A, B dos conjuntos no vacíos tales que $|A| = n$, $|B| = k$ y una aplicación $f : A \to B$.

(a) Entonces, sea cual sea la aplicación f, si $n > k$ existen al menos dos elementos de A, a_1, a_2 ($a_1 \neq a_2$) tales que $f(a_1) = f(a_2)$.

(b) O, en términos más generales, si $n > kr$, para cierto $r \geq 1$, hay al menos $r+1$ elementos distintos de A, $a_1, a_2, \ldots, a_{r+1}$, tales que

$$f(a_1) = f(a_2) = \cdots = f(a_{r+1}).$$

Para probar que $s(p,2) = 4p-3$, primero consideremos las siguientes definiciones.

Definición 1.2. *Un **punto entero** en el plano es un punto de coordenadas enteras; es decir, un punto $P = (x,y) \in \mathbb{Z} \times \mathbb{Z}$*

Definición 1.3. *Dado un conjunto $\mathcal{A} = \{P_1, \ldots, P_k\}$ de k puntos enteros en el plano, donde $P_i = (x_i, y_i) \in \mathbb{Z} \times \mathbb{Z}$, para $i = 1, \ldots, k$, definimos su* **centroide** *ó k-**centroide** como el punto:*

$$\frac{1}{k}\sum_{i=1}^{k} P_i := \left(\frac{1}{k}\sum_{i=1}^{k} x_i, \frac{1}{k}\sum_{i=1}^{k} y_i\right). \tag{1.1}$$

Definición 1.4. *Decimos que un subconjunto no vacío $\mathcal{P}$ de $\mathbb{Z}\times\mathbb{Z}$ tiene k-**centroide entero** si existe $\mathcal{A}=\{P_1,\ldots,P_k\}\subseteq\mathcal{P}$ tal que el centroide de $\mathcal{A}$ es un punto entero. En caso contrario, decimos que $\mathcal{P}$ es libre de k- centroide entero.*

El problema que surge entonces lo podemos describir así: dado k fijo, determinar el menor número entero positivo $s(k,2)$ tal que dados cualquier s puntos enteros en el plano existen k de ellos cuyo centroide también es un punto entero. En consecuencia estudiaremos la función:

$$s(k,2):=\text{mín}\{|\mathcal{P}|:\mathcal{P}\subset\mathbb{Z}\times\mathbb{Z}\text{ y }\mathcal{P}\text{ tiene k-centroide entero}\},\tag{1.2}$$

la cual existe por las cotas triviales (0.1), dadas por H. Harborth [9], tomando en este caso $d=2$ tenemos que $4n-4<s(n,2)\leq(n-1)n^2+1$; así, para la cota inferior, si tomamos una secuencia formada por $n-1$ copias de cada uno de los cuatro puntos

$$(0,0),(0,1),(1,0),(1,1),$$

podemos observar que ninguna de las $\begin{pmatrix}4n-4\\ n\end{pmatrix}$ subsecuencias tiene suma cero. Y para la cota superior si tomamos una secuencia de tamaño $(n-1)n^2+1$ en $\mathbb{Z}_n\oplus\mathbb{Z}_n$, por el Principio del Palomar, un punto debe aparecer al menos n veces. Analicemos la función (1.2) para algunos valores particulares de k; por ejemplo, para el caso de $k=2$, por las cotas triviales dadas en (0.1) tenemos que $s(k,2)=5$.
Ahora estudiemos el caso para $k=3$, el problema consiste entonces en determinar el menor entero $s(3,2)$ que obliga a la existencia de un 3-centroide entero; en la explicación que damos a continuación nos podemos dar cuenta que el problema para este caso se vuelve más complicado pues el Principio del Palomar no es suficiente para la demostración. Primero, consideremos el siguiente conjunto:

$$\mathcal{P}=\{(0,0),(0,3),(0,1),(0,4),(1,0),(4,0),(1,1),(1,4)\}$$

el cual es libre de 3-centroide entero pues tenemos que ninguno de los $\begin{pmatrix}8\\3\end{pmatrix}=56$ subconjuntos de 3 elementos de $\mathcal{P}$ tiene 3-centroide entero, debido a que los modelos módulo 3 componente a componente de los ocho puntos son $\{(0,0),(0,1),(1,0),(1,1)\}$, cada elemento con multiplicidad 2 y a partir de ellos no es posible tener que la suma de tres puntos de $\mathcal{P}$ produzca un modelo de la forma $(0\ mod\ 3, 0\ mod\ 3)$. Así, $s(3,2)>8$.
Sin embargo, tenemos que $s(3,2)=9$ y como lo mencionamos anteriormente, el Principio del Palomar no es suficiente para probar esta afirmación, se necesitan otros argumentos por ejemplo el uso del plano proyectivo como lo describen en el texto [7]. Aquí presentamos una reconstrucción de esta prueba.

Teorema 1.5. *Todo conjunto de puntos enteros en el plano con 9 o más elementos tiene 3-centroide entero.*

Demostración. Sea $\mathcal{P}=\{P_1,\ldots,P_9\}\subseteq\mathbb{Z}\times\mathbb{Z}$, vamos a probar que existen tres puntos de $\mathcal{P}$, $P_i=(x_i,y_i)$, $P_j=(x_j,y_j)$, $P_k=(x_k,y_k)$ con i,j,k en $\{1,\ldots,9\}$ tales que

$$x_i\equiv x_j\equiv x_k(mod\ 3)\text{ o }\{x_i(mod\ 3),x_j(mod\ 3),x_k(mod\ 3)\}=\{0,1,2\},\text{ y}$$

$$y_i\equiv y_j\equiv y_k(mod\ 3)\text{ o }\{y_i(mod\ 3),y_j(mod\ 3),y_k(mod\ 3)\}=\{0,1,2\}.$$

Los nueve posibles puntos enteros módulo 3 distintos, que podemos obtener son todos los elementos de $\mathbb{Z}_3\oplus\mathbb{Z}_3$, los cuales están representados en la siguiente gráfica.

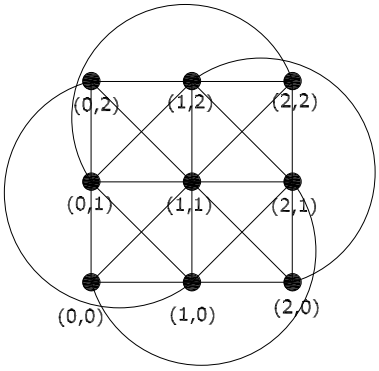

Figura 1: Puntos de $\mathbb{Z}_3 \oplus \mathbb{Z}_3$

Las doce líneas de la Figura 1 corresponden a tripletas de puntos que determinan un 3-centroide entero. Modulando los nueve puntos de $\mathcal{P}$, en módulo 3, pueden suceder los siguientes casos:

- Si tres de los puntos de $\mathcal{P}$ están en la misma clase residual, entonces los tres puntos correspondientes tienen 3-centroide entero.
- Si este no es el caso, supongamos que a lo más dos puntos enteros de $\mathcal{P}$ caen en la misma clase residual, por el Principio del Palomar, tenemos al menos $\lceil \frac{9}{2} \rceil = 5$ puntos en clases residuales distintas. Observemos a continuación que de estos cinco puntos, tres tienen centroide entero, para ello trabajemos con las clases residuales. Por ejemplo, supongamos que tres de estos cinco puntos son $(0,0), (0,1), (1,1)$, que no tienen 3-centroide entero.
  - Si los dos puntos que faltan están en el conjunto $\{(0,2), (2,1), (2,2)\}$ entonces se obtienen puntos colineales y los puntos correspondientes a ellos tienen 3-centroide entero.
  - Si este no es el caso, los dos puntos que faltan pueden ser escogidos de: $\{(1,0), (1,2), (2,0)\}$, pero si escogemos $\{(1,0), (1,2)\}$ ó $\{(1,0), (2,0)\}$ tenemos de nuevo puntos colineales y los puntos correspondientes a ellos tienen 3-centroide entero. O si escogemos $\{(1,2), (2,0)\}$, con el punto $(0,1)$ los puntos correspondientes a ellos tienen 3-centroide entero.

Las demás opciones se prueban análogamente. ☑

2. Valor de la función $s(p,2)$ para $p = 5$

Ahora presentamos una descripción de la prueba del valor de $s(5,2)$ con base en el artículo de Kemnitz [10]. Para ello introducimos la siguiente función $g(p,2)$, la cual es válida para todo entero $p \geq 2$ y se define de la siguiente manera: sea $g(p,2)$ el mínimo cardinal de un conjunto contenido en $\mathbb{Z}_p \oplus \mathbb{Z}_p$, tal que este conjunto contiene un subconjunto de tamaño p cuya suma de elementos es congruente con $(0,0)$ módulo p. Al conjunto con estas características lo

llamaremos conjunto con suma cero; en caso contrario, diremos que el conjunto es libre de suma cero. La existencia de esta función la garantizamos por las cotas triviales

$$2p-1 \leq g(p,2) \leq (p-1)p+1, \text{ para } p \text{ impar.} \tag{2.1}$$

$$2p+1 \leq g(p,2) \leq \frac{1}{2}p(p+1)+4, \text{ para } p \geq 4 \text{ par.} \tag{2.2}$$

Verifiquemos las anteriores cotas para el caso p impar, el otro caso es similar y lo podemos encontrar en [4, 10]. Para la cota inferior de (2.1), veamos algunos ejemplos de conjuntos libres de suma cero.

- Para $p = 3$ el conjunto $\mathcal{P} = \{(0,0),(1,0),(0,1),(1,1)\}$ es libre de suma cero; así, $g(3,2) \geq 5$.
- Para $p = 5$ el conjunto $\mathcal{P} = \{(0,0),(1,0),(2,0),(3,0),(0,1),(1,1),(2,1),(3,1)\}$ es libre de suma cero; así, $g(5,2) \geq 9$.
- Para $p = 7$ el conjunto

  $$\mathcal{P} = \{(0,0),(1,0),(2,0),(3,0),(4,0),(5,0),(0,1),(1,1),(2,1),(3,1),(4,1),(5,1)\}$$

  es libre de suma cero; así, $g(7,2) \geq 13$.

En general, para cualquier $p \geq 3$ impar basta tomar un conjunto con $(p-1)$ puntos cuyas primeras coordenadas (o segundas) sean todas 0 y cuyas segundas coordenadas (o primeras) sean todas diferentes, más $(p-1)$ puntos cuyas primeras coordenadas (o segundas) sean todas 1 y cuyas segundas coordenadas (o primeras) sean todas diferentes. El conjunto con estas características es libre de suma cero, por lo tanto tenemos que $g(p,2) \geq 2p-1$ para todo $p \geq 3$ impar. Para la cota superior de (2.1), tomemos un subconjunto $\mathcal{P} = \{P_1, \ldots, P_{(p-1)p+1}\}$ de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ y consideremos la función $f : \mathcal{P} \to \{0,1,\ldots,p-1\}$ definida por: $f(P_i) = x_i (mod\ p)$, para cada $i = 1,\ldots,(p-1)p+1$. Por el Principio del Palomar al menos $\left\lceil \frac{(p-1)p+1}{p} \right\rceil = \left\lceil (p-1)+\frac{1}{p} \right\rceil = p$ puntos tienen la primera coordenada en la misma clase residual módulo p, digamos que estos puntos son $P_1,\ldots,P_p$. Ahora analicemos la segunda coordenada de estos p puntos, para ello consideremos la función $\tilde{f} : \{P_1,\ldots,P_p\} \to \{0,1,\ldots,p-1\}$ tal que $\tilde{f}(P_i) = y_i (mod\ p)$. Si cada punto tiene distinta imagen, los puntos correspondientes tienen suma cero pues p es impar. Si este no es el caso; es decir, si existe un elemento en el codominio que tiene preimagen vacía, de nuevo por el Principio del Palomar, existen al menos $\left\lceil \frac{p}{p-1} \right\rceil = 2$ puntos que tienen la misma imagen, pero esto no puede ser posible pues todos los puntos de $\mathcal{P}$ son distintos. Por lo tanto, el subconjunto que tiene suma cero es $\{P_1,\ldots,P_p\}$. De otro lado, observemos que la diferencia entre las funciones $s(p,2)$ y $g(p,2)$ es que en la primera se consideran secuencias, es decir, se admiten repeticiones de los elementos; en cambio en la segunda se toman conjuntos. Así, para calcular $g(5,2)$ vamos a tener en cuenta la siguiente terminología: Si p puntos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$ tienen suma cero, llamaremos a esto una ***p-línea*** y dados s puntos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, un ***s-esquema*** consiste de un arreglo de dos filas y s columnas. Esto es, dados $P_1 = (x_1,y_1)$, $P_2 = (x_2,y_2)$, ..., $P_s = (x_s,y_s)$ en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ el s-esquema es el siguiente arreglo

$$\begin{array}{cccc} x_1 & x_2 & \cdots & x_s \\ y_1 & y_2 & \cdots & y_s \end{array}$$

Decimos que dos s-esquemas A y B son *equivalentes* si satisfacen alguna de las siguientes condiciones:

- Si B se obtiene al intercambiar dos columnas o dos filas de A.

- Si B se obtiene al multiplicar una fila de A con $1, 2, \ldots, p-1$.
- Si B se obtiene al agregar a una fila de A el vector $(v, v, \ldots, v)$, de tamaño s.
- Si B se obtiene al sumar una fila con otra de A.

Puede probarse que, dos s-esquemas son equivalentes si y sólo si la existencia de una p-línea en uno de ellos implica una p-línea en el otro y viceversa. Además, para la prueba de $g(5,2)$ usaremos la función $A_p(s,t)$ que representa el mínimo número de sumas incongruentes módulo p, que se obtiene al sumar de cualquier manera s enteros tomados de un conjunto de t enteros incongruentes por pares módulo p, para $1 \leq s \leq t \leq p$. Vale la pena aclarar que no existe ninguna fórmula general para determinar el valor de $A_p(s,t)$ para un primo p arbitrario dado. En la siguiente tabla mostramos los valores de $A_5(s,t)$ cuyos cálculos en detalle se encuentran en [10].

$s \diagdown t$	1	2	3	4	5
1	1	2	3	4	5
2		1	3	5	5
3			1	4	5
4				1	5
5					1

TABLA 1. Función $A_5(s,t)$

Proposición 2.1.

$$g(5,2) = 9. \tag{2.3}$$

Demostración. Sea $\mathcal{P} = \{a_1, \ldots, a_9\} \subseteq \mathbb{Z}_5 \oplus \mathbb{Z}_5$. Por la desigualdad (2.1) para $p = 5$ tenemos que $g(5,2) \geq 9$, por tal razón sólo nos hace falta verificar que 9 es una cota superior; es decir, vamos a verificar que todo 9-esquema contiene una línea. Vamos a ubicar los nueve puntos de $\mathcal{P}$ en un 9-esquema. Si en la primera (o segunda) fila del 9-esquema aparece por lo menos cinco veces un mismoelemento de $\mathbb{Z}_5$ entonces, como los puntos de $\mathcal{P}$ son distintos, las segundas (o primeras) coordenadas de estos puntos son todas diferentes por lo tanto la suma de las correspondientes segundas (o primeras) coordenadas también es congruente con 0 módulo 5. Si este no es el caso, vamos a analizar los 9-esquemas que podemos obtener; por las propiedades de equivalencia de los esquemas nos podemos restringir a 9-esquemas cuya primera fila es alguna de las siguientes. Para $2 \leq a, b, c \leq 4$ tenemos:

(a)	0	0	0	0	1	1	1	1	a
(b)	0	0	0	0	1	1	1	a	a
(c)	0	0	0	0	1	1	1	a	b
(d)	0	0	0	0	1	1	a	a	b
(e)	0	0	0	0	1	1	2	3	4
(f)	0	0	0	1	1	1	a	a	a
(g)	0	0	0	1	1	1	a	a	b
(h)	0	0	0	1	1	1	2	3	4
(i)	0	0	0	1	1	a	a	b	b
(j)	0	0	0	1	1	a	a	b	c
(k)	0	0	1	1	a	a	b	b	c

Ahora, usemos la Tabla 1 y el Teorema de Cauchy-Davenport, Teorema 2.2 en [11], para probar que existe una 5-línea en cada uno de estos casos. Por ejemplo, un esquema puede contener:

- cuatro puntos cuya primera coordenada es 0,
- al menos dos puntos con 1 en la primera coordenada y
- al menos uno con 4 en la primera coordenada.

En este caso, si escogemos de ellos tres puntos con 0, uno con 1 y uno con 4 entonces la suma de las primeras coordenadas de estos cinco puntos es congruente con 0 módulo 5. De los cuatro puntos que tienen primera coordenada 0, de acuerdo al valor $A_5(3,4)$ de la Tabla 1, si sumamos de cualquier manera posible tres de las segundas coordenadas de éstos cuatro puntos, obtenemos como mínimo cuatro clases residuales incongruentes módulo 5; llamemos A el conjunto formado por estas cuatro clases residuales. Como además existen dos posibilidades de escoger 1 en la primera coordenada; llamemos B al conjunto formado por las dos clases residuales de las segundas coordenadas correspondientes a dichos puntos. Ahora formamos el conjunto suma de A y B; por el Teorema de Cauchy-Davenport tenemos que:

$$|A+B| \geq min\{5, |A|+|B|-1\} = 5$$

Es decir, $A+B = \mathbb{Z}_5$. Además, al agregar la clase residual de la segunda coordenada del punto cuya primera coordenada es 4 obtenemos que el residuo 0 también lo podemos representar como suma de las segundas coordenadas; así conseguimos una 5-línea en el 9-esquema y en consecuencia obtenemos la subsecuencia de suma cero. Los demás casos son tratados análogamente, por tal razón omitimos los detalles. ☑

Usando la Proposición 2.1 y el siguiente Lema, debido a J. Olson [12], vamos a mostrar que $s(5,2) = 17$.

Lema 2.2. *Sea p un primo fijo. Toda secuencia de al menos $3p-2$ puntos enteros contiene una subsecuencia de tamaño t, para algún $1 \leq t \leq p$, cuya suma de elementos es congruente con $(0,0)$ módulo p.*

Con base en el artículo de A. Kemnitz en [10] realizamos la prueba del siguiente teorema.

Teorema 2.3. *Todo conjunto de puntos enteros en el plano con 17 o más elementos tiene 5-centroide entero.*

Demostración. Por las cotas triviales dadas en (0.1) es suficiente probar que $s(5,2) \leq 17$. Sea $\{a_1, \ldots, a_{17}\}$ un conjunto de puntos enteros en el plano; si entre los diecisiete puntos encontramos:
Caso 1: Por lo menos cinco puntos que pertenecen a la misma clase residual entonces los puntos correspondientes tienen 5-centroide entero.
Caso 2: Más de ocho puntos tales que por pares sean incongruentes módulo 5 en al menos una coordenada, entonces por la Proposición 2.1 existen cinco de ellos cuyo 5-centroide es entero. Si ninguno de los casos anteriores sucede, nos podemos reducir a trabajar con puntos en $\mathbb{Z}_5 \oplus \mathbb{Z}_5$ y sólo debemos probar la existencia de una 5-línea en el 17-esquema con las siguientes características. Un vector aparece a lo más cuatro veces, por el caso 1; o un vector aparece a lo más $\lceil \frac{17}{8} \rceil = 3$ veces, por el caso 2. Sin perdida de generalidad, por las propiedades de equivalencia de los esquemas, supongamos que ese vector es $(0,0)\,(mod\ 5)$. Entonces tenemos al menos trece puntos diferentes del punto $(0,0)\,(mod\ 5)$; por el Lema 2.2 existen t de ellos, $1 \leq t \leq 5$, cuya suma es congruente con $(0,0)$ módulo 5. Claramente $t > 1$ y si $t = 5$ obtenemos la subsecuencia buscada. Si $2 \leq t \leq 4$, completamos la 5-línea en el 17-esquema con los vectores $(0,0)\,(mod\ 5)$ que ya teníamos. Esto completa la demostración. ☑

Para el caso $p = 7$ no se presentan en este artículo los detalles de la demostración por que son muy extensos, pero se muestran en detalle en [4].

3. La Conjetura de Kemnitz es multiplicativa

Además, podemos notar que la conjetura es multiplicativa; es decir, si la función $s(p,2)$ es verdadera para un par de enteros, también es verdadera para su producto, por tal razón es suficiente verificarla para el caso cuando n es primo, como lo mostramos en el siguiente teorema.

Teorema 3.1. *Si* $n = pq$, $s(p,2) = 4p-3$ *y* $s(q,2) = 4q-3$ *entonces*

$$s(n,2) = 4n-3. \tag{3.1}$$

Demostración. Sea $\mathcal{P} = \{R_1, \ldots, R_{4n-3}\} \subseteq \mathbb{Z} \times \mathbb{Z}$, como $|\mathcal{P}| = 4n-3 = 4pq-3$ y supongamos que $p < q$; escogemos $4q-3$ elementos de $\mathcal{P}$, de ellos existen q puntos, digamos $R_1, \ldots, R_q$, cuyo centroide

$$S_1 = \frac{R_1 + \cdots + R_q}{q}$$

es un punto entero. Sea $\mathcal{P}_1 = \mathcal{P} \setminus \{R_1, \ldots, R_q\}$, así $|\mathcal{P}_1| = 4pq-3-q = (4p-1)q-3$. De los elementos de $\mathcal{P}_1$ escogemos $4q-3$, de ellos existen q puntos, digamos $R_{q+1}, \ldots, R_{2q}$, cuyo centroide

$$S_2 = \frac{R_{q+1} + \cdots + R_{2q}}{q}$$

es un punto entero. Sea $\mathcal{P}_2 = \mathcal{P}_1 \setminus \{R_{q+1}, \ldots, R_{2q}\}$, así $|\mathcal{P}_2| = (4p-1)q-3-q = (4p-2)q-3$ y continuando con el proceso después de $(4p-4)$ pasos nos quedan

$$[4p-(4p-4)]q-3 = 4q-3$$

elementos; de ellos existen q cuyo centroide

$$S_{4p-3} = \frac{R_{(4p-4)q+1} + \cdots + R_{(4p-3)q}}{q}$$

es un punto entero. Ahora, tenemos $4p-3$ puntos enteros, $S_1, \ldots, S_{4p-3}$, de ellos existen p, digamos $S_1, \ldots, S_p$, cuyo centroide

$$\frac{S_1 + \cdots + S_p}{p} = \frac{\frac{R_1+\cdots+R_q}{q} + \cdots + \frac{R_{(p-1)q+1}+\cdots+R_{pq}}{q}}{p} = \frac{R_1 + \cdots + R_{pq}}{pq}$$

es un punto entero. Luego, existen $pq = n$ elementos de $\mathcal{P}$ cuyo n-centroide es un punto entero, los cuales son $R_1, \ldots, R_{pq}$. ☑

El análisis que hicimos anteriormente de algunos valores para la función $s(n,2)$ lo podemos resumir en la siguiente tabla.

n	$s(n,2)$
2	5=4(2)-3
3	9=4(3)-3
5	17=4(5)-3
7	25=4(7)-3

TABLA 3. Algunos valores para la función $s(n,2)$

Con esta información tenemos una conjetura, denominada la Conjetura de Kemnitz, que se enuncia de la siguiente manera:

Conjetura 3.2. *Para todo número entero positivo n tenemos que:*

$$s(n,2) = 4n-3. \tag{3.2}$$

4. Prueba de la Conjetura de Kemnitz

Ahora, presentamos una reconstrucción detallada de la prueba de la Conjetura de Kemnitz, con base en la referencia [13]; primero presentamos tres resultados que tratan de algunas congruencias líneales que relacionan el número de subsecuencias de suma cero de una secuencia dada; su demostración está basada en el Teorema de Chevalley-Warning, Teorema 2.6 en [11] y un lema, debido a N. Alon y M. Dubiner, Lema 3.2 en [1], el cual es una consecuencia del Teorema de Chevalley-Warning.

Teorema 4.1. *(Chevalley-Warning) Sean p un número primo y $\mathbb{F}_q$ el campo finito con $q = p^t$ elementos, donde t es un entero positivo. Para $i = 1, \ldots, m$, sean $P_i(x_1, \ldots, x_n)$ polinomios de grado d_i en n variables con coeficientes en $\mathbb{F}_q$. Si $\sum_{i=1}^{m} d_i < n$ entonces el número N de ceros comunes de $P_1, \ldots, P_m$ (en $\mathbb{F}_q^n$) satisface*

$$N \equiv 0 \,(\text{mod } p). \tag{4.1}$$

En particular, si existe un cero común entonces existe otro.

Lema 4.2. *(Lema N. Alon y M. Dubiner) Sea $a_1, \ldots, a_{3p}$ una secuencia en $\mathbb{Z}_p \oplus \mathbb{Z}_p$ tal que*

$$\sum_{i=1}^{3p} a_i = (0,0). \tag{4.2}$$

Entonces existe un subconjunto $I \subset \{1, \ldots, 3p\}$ con $|I| = p$ tal que

$$\sum_{i \in I} a_i = (0,0). \tag{4.3}$$

La letra X denota una secuencia de elementos de $\mathbb{Z}_p \oplus \mathbb{Z}_p$, el símbolo $N(k, X)$ denota el número de subsecuencias de una secuencia dada $X \subset \mathbb{Z}_p \oplus \mathbb{Z}_p$ de cardinalidad k cuya suma de elementos es divisible entre p (o tiene suma cero). Tenemos entonces las siguientes congruencias lineales.

Corolario 4.3. *Si $|X| = 4p - 3$ entonces*

$$-1 + N(p, X) - N(2p, X) + N(3p, X) \equiv 0 \,(\text{mod } p) \tag{4.4}$$

y

$$N(p-1, X) - N(2p-1, X) + N(3p-1, X) \equiv 0 \,(\text{mod } p). \tag{4.5}$$

Demostración. Sea $X = \{v_1, \ldots, v_{4p-3}\}$, donde $v_i = (a_i, b_i)$, $i = 1, \ldots, 4p-3$. Para la prueba de la congruencia (4.4), consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} x_n^{p-1} = 0, \tag{4.6}$$

$$P_2(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} a_n x_n^{p-1} = 0, \tag{4.7}$$

$$P_3(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} b_n x_n^{p-1} = 0, \tag{4.8}$$

donde P_1, P_2, P_3 en $\mathbb{Z}_p[x_1, \ldots, x_{4p-3}]$. Observe que la suma de los grados de los tres polinomios es $3p-3$, la cual es estrictamente menor que el número de variables $4p-3$, por el

Teorema 4.1 tenemos que el número de soluciones N del sistema satisface $N \equiv 0\,(mod\ p)$. Como el vector nulo es solución del sistema entonces $N > 0$ y N es múltiplo de p, así que: $N \geq p$. Ahora contemos las soluciones no nulas del sistema; el polinomio P_1 se anula en un vector $u = (u_1, \ldots, u_{4p-3})$ con exactamente p, $2p$ ó $3p$ componentes no nulas. Como queremos además que el vector u anule los polinomios P_2 y P_3 entonces el número de vectores u que hacen esto, es:

$$\begin{aligned} N_1 &= (p-1)^p N(p,X) + (p-1)^{2p} N(2p,X) + (p-1)^{3p} N(3p,X) \\ &\equiv -N(p,X) + N(2p,X) - N(3p,X)\,(mod\ p). \end{aligned}$$

Luego, el total de soluciones del sistema es:

$$\begin{aligned} N &= 1 - N(p,X) + N(2p,X) - N(3p,X) \\ &\equiv -1 + N(p,X) - N(2p,X) + N(3p,X) \\ &\equiv 0\,(mod\ p). \end{aligned}$$

La prueba de la congruencia (4.5) es análoga, pero en este caso consideremos el siguiente sistema de polinomios definido por:

$$P_1(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} x_n^{p-1} + 1 = 0, \tag{4.9}$$

$$P_2(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} a_n x_n^{p-1} = 0, \tag{4.10}$$

$$P_3(x_1, \ldots, x_{4p-3}) = \sum_{n=1}^{4p-3} b_n x_n^{p-1} = 0, \tag{4.11}$$

donde P_1, P_2, P_3 en $\mathbb{Z}_p[x_1, \ldots, x_{4p-3}]$. ☑

Las demostraciones de los dos siguientes resultados se encuentran en detalle en [4].

Corolario 4.4. *Si* $|X| = 4p-3$ *entonces*

$$3 - 2N(p-1,X) - 2N(p,X) + N(2p-1,X) + N(2p,X) \equiv 0\,(\text{mod } p). \tag{4.12}$$

Lema 4.5. *(Lema de Reiher) Si* $|X| = 4p-3$ *y* $N(p,X) = 0$ *entonces*

$$N(p-1,X) \equiv N(3p-1,X)\,(\text{mod } p). \tag{4.13}$$

Por último tenemos la demostración de la Conjetura de Kemnitz, hoy Teorema de Kemnitz-Reiher.

Teorema 4.6. *(Teorema de Kemnitz-Reiher) Cualquier secuencia de* $4p-3$ *elementos de* $\mathbb{Z}_p \oplus \mathbb{Z}_p$ *contiene una subsecuencia de cardinalidad* p *y suma cero.*

Demostración. Hagamos la prueba por contradicción. Sea X una secuencia de $4p-3$ puntos enteros del plano y supongamos que ninguna subsecuencia de tamaño p de X tiene suma cero; es decir que $N(p,X) = 0$. Sumando las congruencias (4.4), (4.5) y (4.12) tenemos que

$$\begin{gathered} -1 + N(p,X) - N(2p,X) + N(3p,X) + \\ N(p-1,X) - N(2p-1,X) + N(3p-1,X) + \\ 3 - 2N(p-1,X) - 2N(p,X) + N(2p-1,X) + N(2p,X) = \\ 2 - N(p-1,X) + N(3p-1,X) + N(3p,X) \equiv 0\,(mod\ \text{p}). \end{gathered}$$

Como $N(p,X)=0$ por el Lema 5.5 $N(p-1,X)\equiv N(3p-1,X)\,(mod\ \text{p})$ entonces

$$2-N(p-1,X)+N(3p-1,X)+N(3p,X)=2+N(3p,X)\,(mod\ \text{p}).$$

Así,

$$2+N(3p,X)\equiv 0\,(mod\ \text{p}).$$

Por lo tanto, $N(3p,X)$ debe ser no nulo; luego existe por lo menos una subsecuencia de X de tamaño $3p$ y suma cero; por consiguiente, por el Lema 4.2 existe una subsecuencia de tamaño p y suma cero, en contradicción con la suposición que $N(p,X)=0$. Por lo tanto, $N(p,X)\neq 0$. ☑

5. Conclusiones

Realizamos el estudio en detalle del valor de la función $s(n,2)$ para los casos $n=2,\ 3,\ 5$. Además, se elaboró la reconstrucción de la prueba de la Conjetura de Kemnitz con base en el artículo *On Kemnitz'conjeture concerning lattice-points in the plane.* Ramanujan J., *13:333-337, 2007* de *Christian Reiher*. El aporte que se hace en este trabajo es la ampliación, verificación y descripción en detalle de cada demostración de los resultados dados por el autor C. Rehier.

Aunque se han realizado estudios del problema inicial para dimensiones mayores que dos, solamente se han logrado ciertas cotas para la función $s(n,d)$, con $d>2$; por ejemplo, la cota superior fue mejorada en gran medida por N. Alon y M. Dubiner en [2] probando que $s(n,d)\leq c(d)n$, donde $c(d)$ es una constante independiente de n. Su demostración usa propiedades de expansión de grafos de Cayley y Teoría de Números Aditiva. C. Elsholtz en [5] prueba que la constante $c(d)\geq 2^d 1{,}125^{\lfloor \frac{d}{3} \rfloor}$. Para enteros compuestos $n=n_1n_2$, una cota superior de $s(n,d)$ fue estimada por H. Harborth [9] la cual depende de los valores de $s(n_1,d)$ y $s(n_2,d)$ así:

$$s(n,d)=s(n_1n_2,d)\leq \text{mín}\{s(n_1,d)+(s(n_2,d)-1)n_1, s(n_2,d)+(s(n_1,d)-1)n_2\}.$$

De igual manera, se han realizado muchos estudios sobre el valor de la función $s(n,d)$ para ciertos casos particulares; por ejemplo: $s(3,3)=19$, $s(3,4)=41$, $s(3,5)=91$ y se ha logrado estimar ciertas cotas para $s(3,d)$ con $d\geq 5$, podemos remitirnos a [3, 5, 16].

Referencias

[1] N. Alon and M. Dubiner. *Zero-sum sets of prescribed size.* Combinatorics, Paul Erdös is Eighty, János Bolyai Math Soc., Budapest (1993), 33-50.

[2] N. Alon and M. Dubiner. *A lattice point problem and additive number theory.* Combinatorica 15 (1995), 301-309. János Bolyai Math Soc., Budapest (1993), 33-50.

[3] C. Brewbaker. *Lower Bound Visualization of a Zero-Sum Problem.* Iowa State University (2002).

[4] Y. Caicedo. *Sobre la prueba de la Conjetura de Kemnitz.* Tesis de Maestría en Ciencias Matemáticas. Universidad del Valle. Colombia, (2011).

[5] C. Elsholtz. *Lower bounds for multidimensional zero sum.* Combinatorica 24 (3) (2004), 351-358.

[6] Erdös P., Ginzburg A. and Ziv. A. *Theorem in the Additive Number Theory.* Bull Research Council, Israel 10F (1961), 41-43.

[7] Erickson. M. *Introduction to Combinatorics*. Jhon Wiley & Sons, Inc, United States of America (1963).

[8] Guy. R. *Unsolved Problems in Number Theory*. Springer Science Business Media, Inc, New York, (2004).

[9] Harborth. H. *Ein Extremalproblem für Gitterpunkte*. J. Reine Angew. Math, 262/263 (1973), 356-360.

[10] Kemnitz. A. On a lattice point problem, Ars Combinatorica 16b (1983), 151-160.

[11] Nathanson. M. *Additive Number Theory. Inverse Problems and The Geometry of Sumsets*. Springer-Verlag, New York, 1996.

[12] Olson. J. *A Combinatorial Problem on Finite Abelian Groups I*. Journal Number Theory 1 (1969), 8-11.

[13] Reiher. C. *On Kemnitz'conjeture concerning lattice-points in the plane*. Ramanujan J. 13 (2007), 333-337.

[14] Rónyai. L. *On a Conjeture of Kemnitz*. Combinatorica 20 (2000), 569-573.

[15] Tao and V.H. Vu. *Additive Combinatorics*. Cambridge University Press, New York (2006).

[16] Zhi-Wei Sun. *A Survey of Zero-Sum Problems on Abelian Groups*. Nanjin 210093.

Departamento de Matemáticas
Universidad del Valle
e-mail: yadira0427@gmail.com